REMARKS

Reconsideration and further examination are respectfully requested in view of the above amendments and below remarks.

The Examiner is thanked for the careful consideration and thoughtful remarks in the advisory action. Applicant would like to address the remarks as follows:

1. The Examiner states that the language 'fewer than all' and 'less than all' is not supported by applicant's specification.

In adding this limitation, Applicant was relying on the teaching of the specification at page 10, which states, at lines 12-19":

"... At step 40, upon power reset the contents of the SA table 33 are retrieved from memory 34 and copied to the SA table 36. In addition, the trusted endpoint identifiers are copied to the trusted endpoint table 35. As a result, the SA table 36 stores, at power up, only the SAs for the trusted endpoints; all other endpoints that subsequently request communications with node 30 need to re-negotiate SAs..."

Applicants appreciate that the language does not explicitly state that 'fewer than all' or 'less than all' nodes are added, although they would submit that the meaning is implicit.

However, in order to expedite allowance of the application, Applicants have amended the claims to remove the undesired limitation, and replace the limitation with the language of " only

end-point nodes that are well known to the node and communicate with the node on a regular basis.." No teaching or suggestion of satisfying the 'know' and 'communicate on a regular basis' criteria is shown or suggested by the prior art. Applicants have amended their below arguments in light of the amendment to the claims.

Rejections under 35 U.S.C. §103

Claims 1-20 were rejected under 35 U.S.C. §103 as being unpatentable over Jari et al (U.S. Patent Pub. No. 2001/0020275A1, hereinafter 'Jari') in view of Mercer et al. (U.S. Publication No. 2003/0018908A1, hereinafter 'Mercer').

The Examiner is thanked for the thoughtful examination response that was provided in the last office action. However, it appears that the Examiner did not afford patentable weight to the claims which were newly added in the last response, in particular claims 13, 15 and 18 which clearly stated that the trusted endpoint list identified " less than all of the endpoints that securely communicate with the node…" Applicant's believe that this is a patentable distinction over the combination of references, and did argue such in the last response. The Examiner indicated, at page 5 that 'the features relied upon … were not recited in the rejected claims…' However, applicants respectfully disagree that the limitations could not be found, as claims 13, 15 and 17 clearly recited that the re-use policy limited the number of trusted endpoint to less than the entire trusted endpoint list, and claims 14, 16 and 18 clearly recited that the re-use policy varied with regard to network traffic. Applicant respectfully submits that the Examiner, in the office action, has failed to address the limitations of the new claims when determining patentability of the invention, but rather focused on the applicants argument with regard to the independent claims.

In the interest only of expediting allowance of this case, and not by way of agreement with the Examiner's position, the limitations of dependent claims 13, 15 and 17 have been incorporated into their parent claim. Applicant's would respectfully submit that such an amendment would *not* be a type which would require a new search to be performed by the Examiner, and thus should be allowed in order to place the application in better form for appeal, should the Applicant and the Examiner fail to reach consensus.

The below arguments will now address the distinguishing elements between the Applicant's invention and the combination of prior art references cited by the Examiner.

Jari:

Jari describes, in the Abstract:

"...The security gateway 2 contains a CPU 4 having a volatile memory 5 in which is stored, among other things, a security association database for controlling secure communications between the network and external users. A controller 6 periodically stores the security association database in a disk memory 7 or other nonvolatile memory. When a restoration of power to the security gateway is detected following a power failure, the controller 6 retrieves the latest security association database from the memory 7 and injects it into the volatile memory 5 whose contents were lost during the power failure. The security gateway 2 may then restore secure communication with external users...."

At paragraph [0035] Jari describes:

"...During normal operation of the security gateway 2, the current security association database in the volatile memory 5 is periodically stored in the disk memory 7 by the controller 6. This is illustrated in FIG. 2..."

At paragraph [0037] Jari describes:

"...When power is restored and the security gateway 2 is operative again, the power supply detector 8 supplies a signal illustrated at 20 in FIG. 3 to generate another interrupt 21 for the data processor of the controller 6. At 22, the controller 6 retrieves the most recently stored SAD from the disk memory 7 and, at 23, decrypts the SAD using the latest private key which, for example, may be stored in the disk memory 7 in association with the SAD. The controller 6 may delete expired security associations from the SAD as illustrated at 24 before writing the SAD to the volatile memory 5 as shown at 25. Alternatively, the controller 6 may simply "inject" the whole SAD into the volatile memory of the CPU 4, which then deletes expired security associations. The SAD is thus restored with very little delay and allows the security gateway 2 to begin controlling secure communication between external users and the VPN 1 very quickly. The controller 6 then enters the wait mode as illustrated at 26 and awaits the next interrupt..."

Thus Jari describes a system which backs up and restores an entire database of security associations. Jari is silent as to how the particular security associations are stored in the security associations database, but rather is directed solely at backing up and restoring the database.

Mercer:

Mercer describes a method for establishing a secure communication channel for information flow between two or more computers and a system for implementing the method in response to receiving a security association from one of the computers. [Mercer, Abstract]

In particular, Mercer is concerned with reducing the calculation overhead and processing time associated with establishing and determining Security Associations for inbound IPSec traffic. [Mercer, paragraph 11]

To overcome the problems of the prior art, Mercer assigns SPI values based on the memory location where the Security Association (SA) will reside. For example, as described at paragraph [0029] of Mercer:

"... Each memory region in the memory storage device 514 is, as is generally known, indexed using a specific memory address value. In a preferred embodiment, each memory address value is 32-bits in length, which matches the standard bit length of an IPSec SPI value. Thus, the memory address value of the memory region that will store the SA structure is assigned

as the SPI value 312, 412 of the inbound SA (STEP 610). The IPSec hardware device 510 then writes the inbound SA structure to the assigned memory region for storage (STEP 612), and the IPSec memory management software passes the SPI value 312, 412 to the IKE software component 504 (STEP 614), which maintains its own SA tables. ... The computer 500, via the IKE software component 504, then transmits the assigned SPI value back to the computer that requested that the SA be established (STEP 616). The process then ends (STEP 618). .."

As described at paragraph [0031] of Mercer:

"...The present invention eliminates the need for elaborate and time consuming SAD table lookup algorithms, which result in costly memory access times and complex lookup hardware. The present invention allows high-speed and efficient inbound SA lookup without significantly impacting memory access bandwidth..."

The Examiner alleges that Jari teaches several elements of the claim, but states, at page 4 of the office action:

"... Jari does not explicitly disclose
wherein the set of security associations includes only the security associations for endpoint nodes that are trusted by the node;
receiving, at the node, a communication from the endpoint node
determining whether a security association for the endpoint node is included in the working set of security associations;
responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node..."

However, in the field of endeavor Mercer discloses,
wherein the set of security associations includes only the security associations for endpoint nodes that are trusted by the node; [paragraph 0025]...
receiving, at the node [paragraph 0026 and paragraph 0030] ... a communication from the endpoint node...
determining whether the security association for the endpoint node is included in the working set of security associations [paragraph 0026 and paragraph 0030]...
responsive to a determination that the security association for the endpoint node is in the working set ... using the security association to process the communication from the endpoint node..."

"...It would have been obvious to one of ordinary skill in the art ... to combine the features of including only the security associations for endpoint nodes that are trusted by the node; receiving at the node, a communication from the end point node; determining whether a security association for the endpoint node is included in the working set of security associations;

and responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node as per teachings of Mercer into the method taught by Jari for the purpose of eliminating the need for elaborate and time consuming SAD/ security association databases lookup algorithms, which result in costly memory access times and complex lookup hardware [See Mercer, paragraph 0031]..."

Applicants respectfully disagree.

The Asserted Combination neither discloses of suggests the claimed invention

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Independent claims 1, 5 and 7:

Independent claims 1, 5 and 7 each include limitations which are neither taught nor suggested by the combination of Mercer and Jari. In particular, each of the independent claims are directed to a method or apparatus which identifies trusted end points and maintains security associations only for trusted end-points, where the re-use policy dictates that the list includes *only end-point nodes that are well known to the node and communicate with the node on a regular basis*. For example, claim 1 includes the step of "copying, responsive to a reset at the node, a set of security associations stored in a memory to a working set of security associations, wherein the set of security associations includes only the security associations for...a set of trusted endpoint nodes, the set of trusted endpoint nodes determined according to a security association re-use policy of the node..." Claim 5 recites the step of "...selectively storing

an identifier of the endpoint on a trusted endpoint list according to a re-use policy of the node ..." Claim 7 recites the element of "a list of trusted endpoints, the list of trusted endpoints being determined according to a security association re-use policy of the network device ..."

No such structure is shown or suggested by the combination of Mercer and Jari. The Examiner states that Mercer teaches that the step of 'the set of security associations includes only the security associations for endpoint nodes that are trusted by the node...' is taught by Mercer at paragraph 0025. However, paragraph 0025 merely states:

> "... If the first 110 and second 114 gateway computers already share an IKE SA, then the IPSec SA can be created fairly quickly. If not, then an IKE SA must first be established before an IPSec SA can be established. To establish an IKE SA, the first 110 and second 114 gateway computers exchange digital certificates, which have been digitally signed by a trusted third party certificate authority 115. Thereafter, when the IKE session becomes active, the first 110 and second 114 gateway computers can establish the IPSec SA..."

As best can be understood by the Applicant, it would appear that the Examiner is stating that *any* endpoint that communicates using an IPSec SA is a 'trusted' end point. Applicants have amended the claims to highlight that 'trusted end-points' of the claim are identified according to a security association re-use policy.

The combination of Jari and Mercer does not distinguish between end-points when storing security associations; rather Mercer stores and restores the entire database of security associations. One advantage of identifying trusted end-points is described at page 9 of Applicant's specification, as 'The SA logic 32 takes advantage of the fact that certain endpoints are well known to each node. These endpoints are allowed a very fast but secure method to re-establish communications with the node in the event of a power failure..." Examples of such trusted end points are provided at pages 8 – 9, and include branch offices, telecommuters, etc. As described on page 9, line 5 'Re-use policies can also be flexible depending upon the amount

of traffic the VPN is handling; for example, if the traffic load is light and not many users are using the communications channels, the policy may specify that a full IKE exchange should be used in the event of a power down..." No such advantage may be realized by the combination of Mercer and Jari.

Thus, for at least the reason that the combination of Jari and Mercer fails to describe or suggest every limitation of the claims, it is respectfully requested that the rejection under 35 U.S.C. §103 be withdrawn and the claims allowed to issue.

Dependent claim 2-4, 6 and 7-12 and 14, 16, and 18-20 serve to add further patentable limitations to their parent independent claims and are allowable for at least the same reason as their parent claims. For example, the combination of references neither describes nor suggests 'wherein the re-use policy varies in accordance with network traffic' as recited in claims 14, 16 and 18. Accordingly it is requested that the rejection of these claims be withdrawn.

Conclusion

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

November 8, 2007
Date

/Lindsay G. McGuinness/
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-335
Dd: 9/26/2007